IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Applicant:	Larry H. Gass et al.	§	Art Unit:	2137
Serial No.:	09/922,041	§	Examiner:	Minh Dieu T. Nguyen
Filed:	August 3, 2001	§	Atty Docket:	ITL.0506US (P10475)
For:	Firmware Security Key Upgrade Algorithm	§	Assignee:	Intel Corporation

Mail Stop **Appeal Brief-Patents**
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REPLY BRIEF

In response to the new points raised by the Examiner, the following Reply Brief is submitted.

Claim 40 requires that a first portion of the basic input/output system that is not upgradeable include an upgrade verification code. For the first time on appeal, the Examiner contends that the upgrade verification code described in claim 40 is the validation key that is part of the ROM image.

However, the claim requires that the upgrade validation code be part of the basic input/output system and, specifically, the portion of the basic input/output system that is not upgradeable.

The reference is clear that the basic input/output system is on RAM, not on ROM. See column 7, lines 7-10.

Date of Deposit: August 11, 2008
I hereby certify under 37 CFR 1.8(a) that this correspondence is being deposited with the United States Postal Service as **first class mail** with sufficient postage on the date indicated above and is addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Cynthia L. Hayden

Cynthia L. Hayden

Unlike the claimed invention, the upgrade program in the reference is stored in a separate memory (ROM) from the memory containing the basic input/output system (RAM) to be updated.

Therefore, the reference is not relevant and the rejection should be reversed.

Claim 1 calls for retrieving a second public key from the firmware program if the public key is not valid.

For the first time on appeal, the Answer suggests that the cited reference teaches such an element because the cited reference contemplates the possibility that the manufactured private signature key might simply be lost or destroyed. See paragraph 251. In this case, the key can be reissued. But a lost or destroyed key is not invalid. The reference itself, in the cited paragraph, distinguishes between an invalid key which has been compromised and a key that is still valid and may be reused because it is merely lost or destroyed. Thus, the cited reference has no pertinency to the claimed invention because there is no retrieving of a second public key. The same public key is simply reestablished.

Moreover, this reestablishment of the public key does not occur by retrieving a second public key from the firmware program. Instead, the same public key is simply reissued through the authority of a manufacturer who "could then turn to that trusted third party and request that it issue an instruction data packet to all manufacturer's devices authorizing the replacement of the manufacturer's public key, thus saving itself and its users the potentially huge expensive of physically replacing all the physical devices." See paragraph 251.

As pointed out thereafter, "if the manufactured private key was lost or destroyed, and not compromised, then all previous signatures would still be valid and the user would need only to present his old device certificate in order to have a new device certificate issued for the information signed by the manufacturer's new signature key." [Emphasis added].

Thus, the reference only concerns the situation where the key is still valid and can be reissued. A new or second key is not issued and it is not issued from the firmware program.

For all of these reasons, the cited reference is not pertinent and the rejection should be reversed.

Respectfully submitted,

Date: August 11, 2008

Timothy N. Trop, Reg. No. 28,994
TROP, PRUNER & HU, P.C.
1616 S. Voss Road, Suite 750
Houston, TX 77057
713/468-8880 [Phone]
713/468-8883 [Fax]

Attorneys for Intel Corporation